ISSUE:

- Should the DCI's Letter of promulgation of the COMPUSEC SAFEGUARDS be delayed because of Don Latham's letter of 10 May 1985 to NSA and DIA?

GENERAL CONCERN:

- On 10 May 1985 Don Latham signed out a letter to NSA and DIA (with responses due 31 May 1985) which references the DCI's intent to promulgate the SAFEGUARDS (this DCI action has been in suspense since late February; Dr. Davis spoke to you about it last week. An official letter of promulgation is being developed jointly by C/SECOM, IHC, and Dr. Davis with intentions to send it through you to the DCI for signature some time before 24 May 1985).

- In his letter Don Latham notes that C^3I's preliminary assessment of the SAFEGUARDS suggests some potential problems with regard to implementation within DoD, including some inconsistencies with the DoD Computer Security Center's Evaluation Criteria. He requests a review by NSA and DIA to assess the SAFEGUARDS in terms of: (a) the impact of implementation within DoD and (b) consistency with the DoD Criteria. He requests these responses from NSA and DIA no later than 31 May 1985 so that he will be prepared to discuss the document with the IC Staff.

BACKGROUND:

- The SAFEGUARDS document was distributed on 22 January 1985 to NFIC members and selected government officials with responsibilities assigned [redacted] as part of the three package set that included: the COMPUSEC threat, the technology assessment document, and the SAFEGUARDS document. In this memorandum of transmittal the DCI stated: "I intend to direct that the SAFEGUARDS be imposed as mandatory standards for the 13 'critical' SCI-handling systems by the end of FY86. These SAFEGUARDS will also be imposed as voluntary standards for other SCI-handling systems." STAT

- The SAFEGUARDS document was developed as a result of the DDCI's 6 May 1983 letter to the D/ICS which requested the development of a set of "Community-coordinated minimum acceptable computer security standards" to be applied to any Community computer networks that might be developed. The DDCI's letter suggested using the DoD Computer Security Evaluation Center's criteria as a starting point.

- Per Dr. Davis' recommendation, in a letter of 6 June 1983 D/ICS responded to DDCI that "Formal computer standards require five to seven years to develop, to coordinate, and to introduce effectively into the infrastructure." A dual approach was recommended in the 6 June 1983 D/ICS letter. This dual approach has been the basic format of the COMPUSEC effort. This dual approach is:

-- Set near term priorities for identifying a set of mandatory standards (later termed SAFEGUARDS at the request of the COMPUSEC Steering Group) for a limited number of "critical systems" as a fast track, near term action to reduce the security risks from a set of vulnerabilities which by any criteria generate the greatest threat and highest risk (e.g., access procedures, security labeling, and accountability) to information processed by automated systems.

-- Follow through with this effort in a more deliberate pace, to develop and coordinate the more broadly applicable standard or standards through the existing mechanism of the Computer Security Subcommittee of SECOM. These are intended to cover ALL automated systems processing information derived from sensitive intelligence methods and sources (i.e., not just "critical systems").

o The DDCI concurred with this proposed plan of action and issued supplemental guidance (verbally) that the SAFEGUARDS to be promulgated must be "doable" and we must be able to "identify the cost of implementation".

o During the summer and fall of 1983, a 10 member working group under the auspices of the COMPUSEC effort developed a DRAFT set of SAFEGUARDS which were based primarily on the DoD Computer Security Center's Evaluation Criteria (i.e., 21 of 41 SAFEGUARDS were taken word for word out of the DoD criteria; the remainder covered physical, personnel, and procedural security areas). These were issued in draft form on 17 October 1983.

o These 41 SAFEGUARDS were used as the basis for evaluating the security of the 13 "Critical Systems" and to estimate the costs associated with fixing the identified problems in the "critical systems".

o As a result of the "critical system" assessments, CIA and DIA argued that the DoD Computer Security Criteria and the 41 SAFEGUARDS (which were based on the DoD criteria) were NOT achievable in existing systems and that the cost of retrofiting the systems would be prohibitive. NSA made the same argument via its comments and complete destruction of the CIRS security plan (also based on the DoD CSC's criteria) which included the NSA "critical system" [redacted] As you recall, DIRNSA refused to have his "critical systems" evaluated by anyone outside of NSA as part of the DCI's COMPUSEC effort. STAT

STAT

- Based on the "census type data" that we were able to obtain from security evaluations of the systems at DIA/DoDIIS, CIA, State, and IC Staff, the COMPUSEC project team redrafted the SAFEGUARDS using the recently retired Chief of Computer Security for DIA/DoDIIS, [redacted] as a principal author of the SAFEGUARDS under a contract to the IC Staff. [redacted] had 20 years of experience in this area and was involved in the assessments of ALL of the "critical systems," except NSA systems, just prior to his retirement. He is aware of both cost and implementation issues that were inherent in the 41 SAFEGUARDS issued on 17 October 1983. STAT STAT

- The SAFEGUARDS were redrafted by the COMPUSEC project team and reduced to a total of 29 SAFEGUARDS. Per the suggestions of the organizations involved in the assessments, the SAFEGUARDS were oriented in a scalar fashion to the basic DCID 1/16 modes of operation (i.e., dedicated, system high, and compartmented) so that 14 SAFEGUARDS are mandatory for systems operated in the DCID-defined dedicated mode of operation, 25 SAFEGUARDS are mandatory for systems operated in the system-high mode of operation, and all 29 are mandatory for those systems operated in the compartmented or multi-level security mode of operation. The SAFEGUARDS document was informally coordinated with CIA, DIA, State, and OUSD(P).

- The SAFEGUARDS document addressed specific vulnerabilities identified in the assessments of the 11 "critical systems" in which the authors (primarily [redacted]) were allowed to participate. It was specifically and intentionally written to be consistent with the DoD CSC although (per Dr. Davis' guidance) the SAFEGUARDS attempted to avoid most of the confusing technical jargon that is included in the DoDCSC. STAT

- While the DoDCSC criteria addresses only the technical aspects of automated information systems security, the SAFEGUARDS addresses personnel, physical, procedures, IN RELATION TO THE TECHNICAL CRITERIA. This included the need for formal accreditation BECAUSE NONE OF THE CRITICAL SYSTEMS HAVE BEEN APPROPRIATELY ACCREDITED UNDER THE PROVISIONS OF DCID 1/16.

- DoD has been in involved in an 18 month debate over the DoDCSC criteria which may be resolved in the next 30-90 days with a reissuance of the criteria including some changes that DIA has specifically requested. The criteria will still be limited to "technical" criteria. In addition, the original intent of its development has been diluted to such a point that a whole new set of security criteria are being developed for networks (probably available in late 1985), and now the DoD says it must develop criteria for DBMS which are the main stays of several of the DCI's critical systems. IT IS NOT CLEAR WHAT THE DoD CRITERIA WILL NOW COVER WHEN THEY ARE PROMULGATED.

- Further delays in promulgating the SAFEGUARDS could result in budgetary impacts (i.e., the COMPUSEC money in the NFIP for FY86-FY88 is justified based on the need to fix "critical systems" IAW the SAFEGUARDS).